Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently amended) A method comprising:

~~generating information~~ first monitoring network traffic, and generating an average that relates to traffic of a specified type;

comparing current network traffic to said average, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points ~~from a source and directed to a target device~~, the unwanted communications being of a type ~~adapted~~ to reduce the ability of the target device to respond to other communications; and

based on said comparing analyzing the information generated at the first and second points to identify which of the points first carried the unwanted communications.

2. (Original) The method of claim 1, also including detecting the direction of the unwanted communications.

3. (Original) The method of claim 1, also including identifying the target device.

4. (Cancel).

5. (Cancel).

6. (Original) The method of claim 1, also including correlating communications request messages with acknowledgement messages.

7. (Original) The method of claim 1, also including communicating information about the unwanted communications to brokers.

8. (Original) The method of claim 7, also including communicating information about the unwanted communications among brokers.

9. (Original) The method of claim 1, also including blocking a portion of communications passing through the point through which the unwanted communications originated.

10. (Original) The method of claim 9, also including blocking a portion of communication request messages passing through the point through which the unwanted communications originated.

11. (Original) The method of claim 1, in which the target device comprises a web server.

12. (Currently amended) A method comprising:

monitoring network traffic, and generating an average that relates to traffic of a specified type;

monitoring current communications passing through at least a first point and a second point on a path ~~from a source sub-network to a target device~~ and comparing said current communications with said average;

~~analyzing the communications passing through the first and second points for~~ using said comparing to find indicia of unwanted communications;

~~identifying the source sub-network as originating unwanted communications that are adapted to reduce the ability of a target device on a network to respond to other communications, the source sub-network connected to the network through an interface device associated with the first of the at least a first point and a second point that carried the unwanted communications;~~ and

blocking communications passing through the interface device based on said using.

13. (Original) The method of claim 12, also including blocking a portion of the communications passing through the interface device.

14. (Original) The method of claim 13, also including blocking a portion of communication request messages passing through the interface device.

15. (Canceled).

16. (Canceled).

17. (Canceled).

18. (Canceled).

19. (Previously Presented) The method of claim 12, also including correlating communication request messages passing though the first and second points with acknowledgement messages.

20. (Currently amended) A system comprising:

first and second interface devices for detecting and generating information about current network traffic ~~unwanted communications from a source passing through the first and second interface devices directed to a target device~~; and

a communications analyzer monitoring network traffic, and generating an average that relates to traffic of a specified type, and [[for]] analyzing the information generated at the

first and second interface devices relative to said average to identify unwanted communications, and to identify which of the interface devices first carried the unwanted communications.

21. (Original) The system of claim 20, in which the communications analyzer also includes:

an interface monitor corresponding to each interface device; and

a communications link between the interface monitors.

22. (Cancel).

23. (Original) The system of claim 22, also including an interface coordinator associated with each interface device for instructing the interface devices to block messages.

24. (Currently amended) A system comprising:

a communications monitor for detecting and generating information about unwanted messages originating on a first network and directed to a target device on a second network, the communications monitor comprising:

a plurality of interface monitors between the first network and the second network for monitoring the passage of unwanted messages therethrough;

monitoring network traffic, and generating an average that relates to traffic of a specified type;

a localizer coupled to the plurality of interface monitors to identify the network point that first carried the unwanted messages by comparing current network traffic with said average; and

a gating module for blocking messages passing through the network point identified by the localizer from the first network to the second network.

25. (Canceled).

26. (Canceled).

27. (Previously Presented) The system of claim 24, in which the communications monitor also includes a statistics analyzer for statistically analyzing the messages passing through the plurality of points.

28. (Original) The system of claim 24, in which the gating module is operable to block a portion of the messages passing from the first network to the second network.

29. (Original) The system of claim 28, in which the gating module is operable to block a percentage of all messages passing from the first network to the second network.

30. (Original) The system of claim 28, in which the gating module is operable to block a portion of communication request messages directed to the target device.

31. (Currently amended) A computer program embodied in a computer readable medium, the program capable of configuring a computer to:

monitor network traffic, and generate an average that relates to traffic of a specified type;

generate information by comparing current network traffic with said average, at first and second points of a network, about unwanted communications from a source passing through the first and second points directed to a target device that are adapted to reduce the ability of the target device to respond to other communications; and

analyze the information generated at the first and second points to identify which of the points first carried the unwanted communications.

32. (Original) The program of claim 31, also capable of configuring a computer to block a portion of the communications passing through the point that first carried the unwanted communications.

33. (Currently amended) A computer program embodied in a computer-readable medium, the program capable of configuring a computer to:

monitor network traffic, and generate an average of traffic of a specified type;

generate information by comparing current network with said average, at first and second points of a network, about unwanted communications from a source passing through the first and second points directed to a target device that are adapted to reduce the ability of the target device to respond to other communications; and

analyze the information generated at the first and second points to identify which of the points first carried the unwanted communications.

34. (Currently amended) The program of claim 33, wherein said program is also capable of configuring a computer to block a portion of the communications passing through the point that first carried the unwanted communications.

35. (New) A method as in claim 1, wherein said network traffic of a specified type is a number of SYN requests.

36. (New) A method as in claim 1, wherein said average is a moving average related to the specified type of network traffic.

37. (New) A method as in claim 12, wherein said network traffic of a specified type is a number of SYN requests.

38. (New) A method as in claim 12, wherein said average is a moving average related to the specified type of network traffic.

39. (New) A system as in claim 20, wherein said network traffic of a specified type comprises a number of SYN requests.

40. (New) A system as in claim 39, wherein said average is a moving average related to the specified type of network traffic.

41. (New) A system as in claim 24, wherein said network traffic of a specified type comprises a number of SYN requests.

42. (New) A system as in claim 24, wherein said average is a moving average related to the specified type of network traffic.

43. (New) A program as in claim 31, wherein said wherein said network traffic of a specified type comprises a number of SYN requests.

44. (New) A program as in claim 31, wherein said average is a moving average related to the specified type of network traffic.

45. (New) A program as in claim 33, wherein said wherein said network traffic of a specified type comprises a number of SYN requests.

46. (New) A program as in claim 33, wherein said average is a moving average related to the specified type of network traffic.